ÉMULATION (SANS REDIRECTION)

PAIEMENT EN LIGNE

Nom de fichier : Monetico_Paiement_Internet_Emulation_v2.1
Numéro de version : 2.1
Date : 2017-07-04

Confidentiel

Titre du document : Monetico Paiement Emulation (sans redirection)
Nom de fichier : Monetico_Paiement_Internet_Emulation_v2.1
Numéro de version : 2.1
Date : 2017-07-04

Site Web : www.desjardins.com

TABLE DES MATIÈRES

1 Introduction

1.1 À propos de ce document

L'objectif de ce document est de présenter les aspects techniques de l'intégration en mode émulation (sans redirection) de la solution de paiement en ligne Monetico Desjardins avec votre site commerçant.

1.2 Public cible

Ce document a été rédigé principalement à l'intention des ressources techniques responsables de l'intégration de la solution de paiement en ligne Monetico.

1.3 Terminologie

Le tableau suivant contient un lexique de certains termes utilisés dans le présent document.

Terme utilisé	Terme Desjardins
annulation	annulation d'achat, renversement de préautorisation
appel « phonie »	appel pour autorisation
autorisation	préautorisation
capture de paiement	conclusion de préautorisation
carte bancaire, CB	carte de paiement
chiffre vérificateur	code de vérification
code société	numéro de marchand
commerçant	Marchand
email, mail	Courriel
emails jetables	liste noire (« black list »)
émulation	sans redirection
environnement de validation	environnement de test
interface retour	confirmation
mise en recouvrement	conclusion de préautorisation,
paiement différé	paiement de préautorisation
paiement en attente	paiement en attente
paiement immédiat	paiement d'achat
première échéance	premier versement
recrédit	remboursement
remise	dépôt
société	Entreprise
TPE - Terminal de Paiement Électronique	TPV Terminal Point de Vente; mode de paiement
TPEV - TPE virtuel (web)	TPV virtuel

2 Service d'émulation

2.1 Principe

Le but du service d'émulation de TPEV (Terminal de Paiement Electronique Virtuel) via Internet est de permettre aux commerçants de traiter leurs paiements de façon sécurisée via Internet. Le serveur de paiement de Monetico effectue la vérification de la validité des informations de la carte de paiement transmises avant d'accorder l'autorisation de paiement et confirme automatiquement le résultat de la demande de paiement à l'application du commerçant.

L'application du commerçant dialogue directement avec le serveur de paiement de Monetico. Les échanges se passent en mode sécurisé (cryptage TLS) garantissant la confidentialité des informations fournies par le commerçant.

Afin de certifier les données échangées, un sceau est calculé sur l'ensemble des données fournies par le commerçant au serveur Monetico, à l'aide d'une fonction standard (IETF RFC2104). Ce sceau est intégré aux données fournies et vérifié par nos serveurs à chaque paiement.

2.2 Clé de sécurité commerçant

Une clé de sécurité, propre à chaque TPE, destinée à certifier les données échangées entre le serveur du commerçant et le serveur de paiement de Monetico, est indispensable pour utiliser le service d'émulation de TPEV. Un lien, permettant de télécharger cette clé de sécurité, est envoyé par notre centre de support au commerçant.

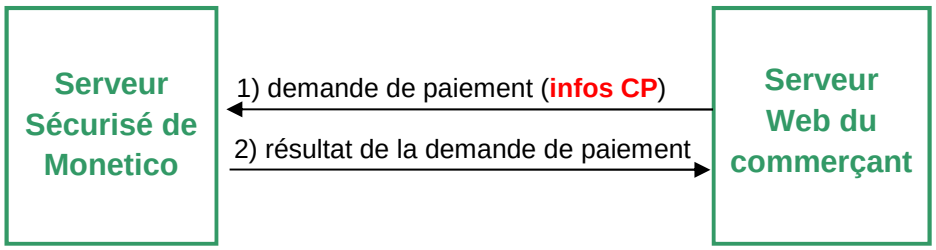
Le commerçant peut demander la régénération d'une nouvelle clé, périodiquement ou à l'occasion d'évènements tels qu'une mise en production, un changement d'hébergeur, un changement de prestataire, etc. Il est de la responsabilité du commerçant de conserver cette clé de façon sûre et confidentielle en exploitant les meilleurs outils disponibles dans son environnement.

La clé de sécurité est représentée de façon externe par 40 caractères hexadécimaux (par exemple : `0123456789ABCDEF0123456789ABCDEF01234567`). Cette représentation externe doit être convertie en une chaîne de 20 octets (représentation opérationnelle) avant utilisation.

2.3 Protocole

2.3.1 Si la carte du client n'est pas 3DSecure

Le schéma suivant décrit les échanges entre le serveur Web du commerçant et le serveur sécurisé de Monetico :

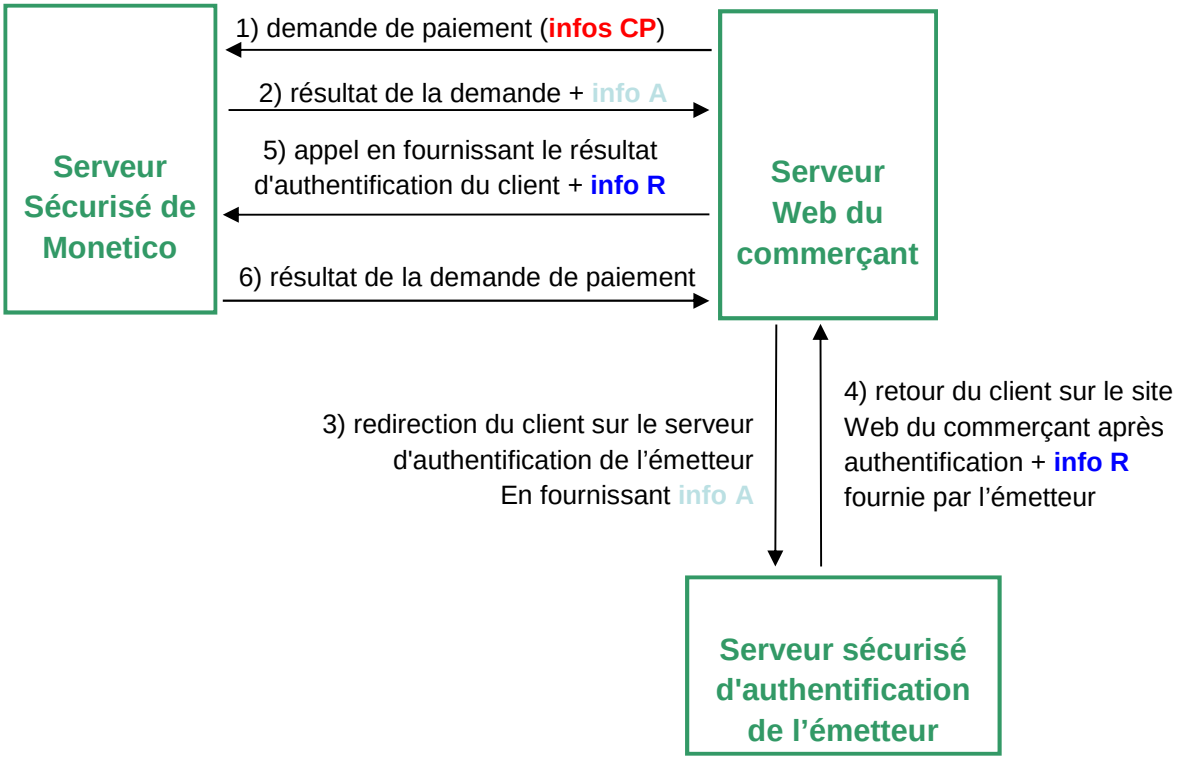


1. Demande de paiement : l'application du commerçant adresse une demande de paiement au serveur Monetico (appel au service d'émulation de TPEV).

2. Le serveur Monetico retourne le résultat de la demande de paiement à l'application du commerçant : paiement accepté ou paiement refusé.

2.3.2 Si la carte du client est 3DSecure

Le schéma suivant décrit les échanges entre le serveur Web du commerçant, le serveur sécurisé de Monetico et le serveur sécurisé d'authentification de l'émetteur de la carte :



1. Demande de paiement : l'application du commerçant adresse une demande de paiement au serveur Monetico (premier appel au service d'émulation de TPEV).

2. Le serveur Monetico retourne, à l'application du commerçant, une demande complémentaire d'authentification du détenteur, contenant l'adresse du serveur sécurisé d'authentification de l'émetteur de la carte ainsi qu'une information (A) à lui transmettre.

3. L'application du commerçant redirige le client vers le serveur d'authentification de l'émetteur de sa carte pour que celui-ci s'authentifie (en fournissant les éléments (A) renvoyés par le serveur Monetico à l'étape 2).

4. Après authentification, le client est redirigé vers le site Web du commerçant accompagné de la réponse (R) du serveur sécurisé d'authentification de l'émetteur de la carte.

5. Le serveur Web du commerçant soumet alors au serveur Monetico le résultat (R) d'authentification du client, tel qu'il a été fourni par l'émetteur de la carte du détenteur (second appel au service d'émulation de TPEV).

6. Le serveur Monetico retourne le résultat du paiement à l'application du commerçant : paiement accepté ou paiement refusé.

3 Spécifications des messages échangés

3.1 Etape 1 : premier appel de l'émulation de TPEV

Les informations de la demande de paiement sont envoyées au serveur Monetico par un message HTTPS (TLS). L'application du commerçant doit émettre une requête en méthode POST à destination du service Emulation de TPEV sur les serveurs Monetico, contenant les champs suivants :

Champs	Description	Remarque
version	Version du système de paiement utilisée	**Version actuelle** `3.0`
TPE	Numéro de TPE Virtuel du commerçant Taille : 7 caractères	**Exemple :** `1234567`
date	Date de la commande au format `JJ/MM/AAAA:HH:MM:SS`	**Exemple :** `05/12/2006:11:55:23`

montant	Montant total incluant les taxes de la commande formatée de la manière suivante :
	Un nombre entier
	Un point décimal (optionnel)
	Un nombre entier de 2 chiffres (optionnel)
	Une devise sur 3 caractères alphabétiques ISO4217 (`CAD`)
		Exemples : `62.73CAD`
		`10CAD`
		`1024CAD`
		
		Attention : un arrondi est effectué automatiquement s'il y a plus de 2 décimales.

reference	Référence unique de la commande Taille : 12 caractères alphanumériques maximum	**Exemple :** `ABERTYP00145`
texte-libre	Zone de texte libre Taille : 3200 caractères maximum	
lgue	Code langue (en majuscules) Taille : 2 caractères	`FR ou EN`
societe	Code alphanumérique permettant au commerçant d'utiliser le même TPE Virtuel pour des sites différents (paramétrages distincts) se rapportant à la même activité	**Ce code est fourni par nos services.** **Exemple :** `monSite1`
MAC	Sceau issu de la certification des données Taille : 40 caractères hexadécimaux	
numero_carte	Numéro de la carte du détenteur	**Ex :** `1234567890123456`
annee_validite	Année d'expiration de la carte Taille : 4 chiffres	**Exemple :** `2008`
mois_validite	Mois d'expiration de la carte Taille : 2 chiffres	**Exemple :** `08`
cvx	Cryptogramme visuel de la carte du détenteur	**Exemple :** `123` **Ce paramètre est optionnel pour certaines cartes**

phonie	La valeur de ce champ sera renvoyée en cas d'appel phonie	**Ce paramètre est optionnel**
Mail	Email de l'internaute	**Ex : dupont@yahoo.ca**
options	Liste des options utilisées (peut être vide). Chaque option est séparée des autres par un caractère '&'. Si l'option a une valeur, le nom est séparé de la valeur par le caractère '='.	**Exemple :** `clientip=10.20.30.40&detailrefus=1`

3.1.1 Appel Phonie

Il est possible qu'une demande d'autorisation soit refusée pour un motif du type « appel phonie » (montant trop élevé, centre d'autorisation encombré, etc.).
Il peut alors être nécessaire pour le commerçant de faire une demande manuelle (téléphone, fax) au centre d'autorisation du détenteur de la carte, qui communiquera en retour des coordonnées bancaires et du montant, un numéro d'autorisation pour cette transaction.
Remarque : Cette fonction n'est pas actuellement offerte par Desjardins.

3.1.2 Liste des options possibles

Options	Description	Remarque
aliascb	Alias de la carte de paiement d'un client en cas de souscription de l'option « paiement express » Format : [a-zA-Z0-9]{1,64}	**Exemple :** `aliascb=client1`
clientip	Adresse IP du client Format : 0-255.0-255.0-255.0-255	**Exemple :** `clientip=10.20.30.40`
detailrefus	Si activée et en cas de refus : permet de distinguer les différentes causes de refus dans un champ dédié. Valeurs autorisées : 0 : option inactive (valeur par défaut) 1 : option active	**Exemple :** `detailrefus=0`

Remarque :

Lorsque le nom ou la valeur de l'option ne fait pas partie de la liste des options définies, l'option est ignorée.

3.1.3 Liste des champs propres au paiement fractionné

Champs	Description	Remarque
nbrech	Nombre d'échéances pour cette commande (entre 2 et 4 maximum)	**Exemple :** 4
dateech1	Date de la première échéance au format JJ/MM/AAAA La première échéance correspond à la date de la commande.	**Exemple :** 25/04/2008
montantech1	Montant total incluant taxes de l'échéance formatée de la manière suivante : Un nombre entier Un point décimal (optionnel) Un nombre entier de 2 chiffres (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (CAD)	**Exemples :** 62.73CAD 10CAD 1024CAD ***Attention : un arrondi est effectué automatiquement s'il y a plus de 2 décimales.**
dateech[N] (N entre 2 et 4)	Date de la Nième échéance au format JJ/MM/AAAA	**Exemple :** 05/06/2008
montantech[N] (N entre 2 et 4)	Montant TTC de la Nième échéance formatée de la manière suivante : Un nombre entier Un point décimal (optionnel) Un nombre entier de 2 chiffres (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (CAD, CAD, CAD, CHF, etc.)	**Exemples :** 62.73CAD 10CAD 1024CAD ***Attention : un arrondi est effectué automatiquement s'il y a plus de 2 décimales**

Remarque :

- Pour pouvoir utiliser ces champs, votre TPE doit être configuré pour accepter les paiements en N fois.
- Tous ces champs sont obligatoires
- La somme des montants de chaque échéance doit être égale au montant de la commande.
- Les montants doivent être dans la même devise.
- Les échéances doivent être mensuelles

3.1.4 Calcul du sceau

Le sceau (à mettre dans le champ MAC) est calculé à l'aide d'une fonction de hachage cryptographique en combinaison avec une clé secrète respectant les spécifications de la RFC 2104.

Cette fonction générera le sceau à partir de données à certifier et de la clé de sécurité commerçant sous sa forme opérationnelle.

Les données à certifier seront présentées sous la forme d'une concaténation dans un ordre précis des informations du formulaire :

```
<TPE>*<date>*<montant>*<reference>*<texte-libre>*
<version>*<lgue>*<societe>*<mail>*<nbrech>*<dateech1>*<monta
ntech1>*<dateech2>*<montantech2>*<dateech3>*<montantech3>*<d
ateech4>*<montantech4>*<options>
```

Exemple pour un paiement :

```
1234567*05/12/2006:11:55:23*62.73CAD*ABERTYP00145*ExempleT
exteLibre*3.0*FR*monSite1*internaute@sonemail.ca**********
```

Exemple pour un paiement fractionné :

```
1234567*05/12/2006:11:55:23*62.73CAD*ABERTYP00145*Exemple
TexteLibre*3.0*FR*monSite1*internaute@sonemail.ca*4*05/12/
2006*16.23CAD*05/01/2007*15.50CAD*05/02/2007*15.50CAD*05/0
3/2007*15.50CAD*
```

3.1.5 Exemple de requête de paiement classique

```
POST /emulation3ds.cgi HTTP/1.0
Pragma: no-cache
Connection: close
User-Agent : AuthClient
Host: p.monetico-services.com
Accept: */*
Content-type: application/x-www-form-urlencoded
Content-length: 301

        version=3.0
        &TPE=1234567
        &date=05%2F12%2F2006%3A11%3A55%3A23
        &montant=62.73CAD
        &reference=ABERTPY00145
        &texte-libre=ExempleTexteLibre
        &lgue=FR
        &societe=monSite1
        &mail=internaute@sonemail.ca
        &MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
```

&numero_carte=1234567890123456
&annee_validite=2008
&mois_validite=08
&cvx=123

3.1.6 Exemple de requête de paiement fractionné (en 2 fois)

```
POST /emulation3ds.cgi HTTP/1.0
Pragma: no-cache
Connection: close
User-Agent : AuthClient
Host: p.monetico-services.com
Accept: */*
Content-type: application/x-www-form-urlencoded
Content-length: 392

version=3.0
&TPE=1234567
&date=05%2F12%2F2006%3A11%3A55%3A23
&montant=100CAD
&reference=ABERTPY00145
&texte-libre=ExempleTexteLibre
&lgue=FR
&societe=monSite1
&mail=internaute@sonemail.ca
&MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
&numero_carte=1234567890123456
&annee_validite=2008
&mois_validite=08
&cvx=123
&nbrech=2
&dateech1=05%2F12%2F2006
&montantech1=20CAD
&dateech2=12%2F01%2F2007
&montantech2=80CAD
```

3.1.7 Réponse de la demande de paiement

L'émulation de TPEV renvoie au commerçant un message au format XML (cf. paragraphe "Message de retour XML" pour la description des balises du message).

La balise <cdr> du message de retour va conditionner la suite du traitement à effectuer :

Valeur de <cdr>	Comportement à adopter	Exemple de message retour
0	Le paiement a été refusé. Il n'est pas nécessaire d'effectuer les étapes 2 et 3, la carte utilisée n'étant pas enrôlée 3DSecure	<xml> <cdr>0</cdr> <version>2.0</version> <reference>reference1</reference> <veres>N</veres> <originecb>CAN</originecb> <hpancb>74E94B03C22D786E0F2C2CADBFC1C00B004B7C45</hpancb> </xml>
1	Le paiement a été autorisé. Il n'est pas nécessaire d'effectuer les étapes 2 et 3, la carte utilisée n'étant pas enrôlée 3DSecure	<xml> <cdr>1</cdr> <version>2.0</version> <reference>reference1</reference> <aut>658745</aut> <veres>N</veres> <originecb>CAN</originecb> <hpancb>74E94B03C22D786E0F2C2CADBFC1C00B004B7C45</hpancb> </xml>
2	La carte utilisée pour effectuer le règlement de la transaction est enrôlée 3DSecure. Le processus doit continuer à l'étape 2	<xml> <cdr>2</cdr> <version>2.0</version> <reference>reference1</reference> <md>B8AAFC7A508DA43FA5AFC474CE71A67697EED</md> <veres>Y</veres> <urlacs>http://url-acs-client/acs.cgi</urlacs> <pareq>IT8ubu+5z4YupUCOEHKsbiPep8UzIAcPKJEjpwGlzD8H0iGQRauaas9dX65ghj321rty63ffhg632r65ghj321rty63ffhMLODtyghjEHKsbiPep8UzIAcPKJEjpwGlzD8HEHKsbiPep8UzIAcPKJEjpwGlzD8HrypeUCOEHKsbiPdfg5jh8353213ert5ezerAcPKJEjpwGlzD8H0iGQRauaas9dX65ghjEjpwGlzD8HEHep8UzIAcPKJKJEjpwGlzghetrzerzteer </pareq> <originecb>CAN</originecb> <hpancb>74E94B03C22D786E0F2C2CADBFC1C00B004B7C45</hpancb> </xml>
< 0	La requête d'émulation a rencontré une erreur. (cf. chapitre « Message de retour XML – Liste des valeurs du code retour dans les messages XML »)	<xml> <cdr>-2</cdr> <version>2.0</version> <reference>reference1</reference> </xml>

3.2 Etape 2 : phase d'authentification du client

Dans le cas où la carte de paiement est 3DSecure, le commerçant devra rediriger le client, à l'aide d'un formulaire employant la méthode POST, sur l'URL (fournie dans la balise <urlacs>) du serveur d'authentification de l'émetteur de sa carte. Le formulaire devra comporter les champs suivants :

Champ	Description
PaReq	récupéré tel quel de la balise <pareq> du message de retour de l'étape 1
MD	récupéré tel quel de la balise <md> du message XML de retour de l'étape 1
TermUrl	URL de retour sur le site du commerçant après authentification du client sur le serveur d'authentification de l'émetteur de sa carte. L'URL de retour doit être une URL complète (par exemple http://marchand.url-retour.com).

Exemple de formulaire:

```
<form name="formulaire" action="http://url-acs-client/acs.cgi" method="post">
        <input type="hidden" name="PaReq"
                value="IT8ubu+5z4YupUCOEHKsbiPep8UzIAcPKJlzD8H0iGQRauaas9dX65ghj321rt
                y63ffhg632r65ghj321rty63ffhMLODrtyghjEHKsbiPep8UzIAcPKJEjpwGlzD8HEHKsbiP
                ep8UzIAcPKJEjpwGlzD8HrypeUCOEHKsbiPdfg5jh8353213587ert5ezer">
        <input type="hidden" name="TermUrl" value="http://marchand.url-retour.com">
        <input type="hidden" name="MD" value=" B8AAFC7A508DA43FA5AFC474CE71A67697EED">
        <input type="submit" value="Cliquez ici pour vous authentifier sur le serveur de l'émetteur">
</form>
```

Quand le client clique sur le bouton de soumission contenu dans le formulaire, il arrive sur le serveur d'authentification de l'émetteur de sa carte et s'authentifie.

3.2.1 Réponse de l'émetteur de la carte

Le serveur d'authentification de l'émetteur de la carte construit un résultat d'authentification et le soumet à l'URL qui a été fournie dans le champ "**TermUrl**" du formulaire (le client est donc à nouveau sur le site du commerçant). Il s'agit d'une requête http en POST, avec les paramètres suivants :

Champ	Description
PaRes	Résultat de la requête d'authentification du client
MD	Donnée permettant d'identifier de manière unique une commande

Exemple de retour :

pares=FDG8p5z4YupUCOEHKsbiPep8UzIAcPKJEjpwGlzD8H0iGQRauaas9dX65ghj321rty63ffhg632r65ghj321rthDio+5kn2Pep8UzIAcPKJEjpwGlzD8HEHKsbiPep8UzIAcPKJEjpwGlzD8HrypeUCOEHKsbiPdfg5jh8353213ert5ezerAcPKJEjpwGlzD8H0iGQRauaas9dX65ghjEjpwGlzD8HEHep8UzIAcPKJKJEjpwGlzghetrzewQ/xc45fr=&md=B8AAFC7A508DA43FA5AFC474CE71A67697EED

Les informations de ce message retour vont être utilisées pour effectuer un second appel du service d'émulation TPE.

3.3 Etape 3 : deuxième appel de l'émulation de TPEV

Le commerçant doit faire un deuxième appel à l'émulation de TPEV en fournissant tel quel le résultat d'authentification reçu de l'émetteur de la carte.

Champ	Description
PaRes	Récupéré tel quel du paramètre « pares » de la requête http du retour de l'étape 2
MD	Récupéré tel quel du paramètre « md » de la requête http du retour de l'étape 2

L'émulation de TPEV effectue alors la demande d'autorisation et renvoie au commerçant un message au format XML contenant le résultat du paiement (paiement accepté ou paiement refusé).

3.3.1 Exemple de requête

```
POST /emulation3ds.cgi HTTP/1.0
Pragma: no-cache
Connection: close
User-Agent : AuthClient
Host: p.monetico-services.com
Accept: */*
Content-type: application/x-www-form-urlencoded
Content-length: 317

        PaRes=
        FDG8p5z4YupUCOEHKsbiPep8UzIAcPKJEjpwGlzD8H0iGQRauaas9dX65ghj321rty
        63ffhg632r65ghj321rthDio%2B5kn2Pep8UzIAcPKJEjpwGlzD8HEHKsbiPep8UzIAcP
        KJEjpwGlzD8HrypeUCOEHKsbiPdfg5jh8353213ert5ezerAcPKJEjpwGlzD8H0iGQR
        auaas9dX65ghjEjpwGlzD8HEHep8UzIAcPKJKJEjpwGlzghetrzewQ%2Fxc45fr%3D
        &MD= B8AAFC7A508DA43FA5AFC474CE71A67697EED
```

Remarques :

Le champ PaRes à renvoyer au serveur Monetico peut contenir des caractères non alphanumériques (‘=’, ‘+’, ‘/’), il faut donc les encoder en respectant le format défini par la RFC 1738 (respectivement ‘%3D’, ‘%2B’, ‘%2F’).

Les exemples précédents utilisent volontairement un champ PaRes avec une taille de données réduite. La taille des données pour le champ PaRes avoisine généralement les 4 Ko.

3.3.2 Message de retour

L'émulation de TPEV renvoie au commerçant un message au format XML (cf. paragraphe "Message de retour XML" pour la description des balises du message).

La balise <cdr> du message de retour contient le résultat de l’authentification du client et de l’autorisation de paiement :

Valeur de <cdr>	Comportement à adopter	Exemple de message retour
0	Le paiement a été refusé. Les raisons du refus peuvent être liées à un échec d’authentification du détenteur (pares=N) ou à un refus d’autorisation du paiement (pares=Y)	<xml> <cdr>0</cdr> <version>2.0</version> <reference>reference1</reference> <veres>Y</veres> <pares>N</pares> <originecb>CAN</originecb> <hpancb>74E94B03C22D786E0F2C2CADBFC1C00B004B7C45</hpancb> </xml>
1	Le paiement a été autorisé	<xml> <cdr>1</cdr> <version>2.0</version> <reference>reference1</reference> <aut>658745</aut> <veres>Y</veres> <pares>Y</pares> <originecb>CAN</originecb> <hpancb>74E94B03C22D786E0F2C2CADBFC1C00B004B7C45</hpancb> </xml>
< 0	La requête d’émulation a rencontré une erreur. (cf. chapitre « Message de retour XML – Liste des valeurs du code retour dans les messages XML »)	<xml> <cdr>-2</cdr> <version>2.0</version> <reference>reference1</reference> <veres>Y</veres> <pares>Y</pares> </xml>

3.4 Message de retour XML

Voici la description des balises des messages XML renvoyés au commerçant :

La partie suivante décrit le cas où l'option « detailrefus » n'est pas utilisée. Si l'option « detailrefus=1 » a été envoyée, se référer directement à la partie « Cas où l'option « detailrefus » est activée ».

3.4.1 Cas classique où l'option « detailrefus » n'est pas activée

Balise	Description	Remarque
<cdr>	code retour	notez bien que si <cdr> est différent de 1, le paiement n'a pas été effectué
<version>	numéro de version du message de retour de l'émulation	Version courante 2.0 (3.0 si module antifraude activé)
<reference>	référence de la commande	
<aut>	numéro d'autorisation	<aut> n'est présent que si le paiement a été accepté
<phonie>	autorisation refusée pour un motif du type "appel phonie"	<phonie> n'est présent que si le champ "phonie" était présent et renseigné dans la requête appelante **Cette fonction n'est pas actuellement supportée par Desjardins**.
<veres>	résultat d'enrôlement 3D-Secure Y : carte enrôlée 3D-Secure N : carte non enrôlée 3D-Secure U : problème technique	
<pares>	résultat d'authentification du client sur le serveur d'authentification de l'émetteur de sa carte Y : client authentifié N : client non authentifié A : la demande d'authentification a été effectuée et l'émetteur assume	<pares> n'est présent que si le commerçant a effectué un deuxième appel à l'émulation TPE suite à l'authentification du client

	l'authentification du client U : non authentifié suite à un problème technique	
<pareq>	message complet à envoyer tel quel au serveur d'authentification de l'émetteur de la carte, pour l'authentification du client	<pareq> n'est présent que si le code retour <cdr> est égal à 2
<urlacs>	URL du serveur d'authentification de l'émetteur de la carte	<urlacs> n'est présent que si le code retour <cdr> est égal à 2
<md>	"Merchant Data" : le commerçant devra fournir telle quelle cette valeur au serveur d'authentification de l'émetteur de la carte.	<md> n'est présent que si le code retour <cdr> est égal à 2
<originecb>	Code pays de l'émetteur de la carte de paiement (norme ISO 3166-1)	<originecb> est présent pour un <cdr> positif ou nul
<hpancb>	Hachage irréversible (HMAC-SHA1) du numéro de la carte de paiement utilisée pour effectuer le paiement (identifiant de manière unique une carte de paiement pour un commerçant donné)	<hpancb> est présent pour un <cdr> positif ou nul
<filtrage>	Informations liées au filtrage du paiement	Uniquement présent lorsque le paiement a été bloqué
<scoring>	Informations liées au scoring du paiement	Uniquement présent lorsque le scoring est activé
<analyse>	Détails du blocage	Un groupe présent pour chaque filtre bloquant le paiement. Entre les balises <filtrage> ou <scoring>
<cause>	Numéros des types de filtres bloquant le paiement (cf. tableau « Retours Module Prévention Fraude – détails » ci-dessous) 1 : Adresse IP 2 : Numéro de carte 3 : BIN de carte	Entre les balises <analyse>

	4 : Pays de la carte 5 : Pays de l'IP 6 : Cohérence pays de la carte / pays de l'IP 7 : Liste noire 8 : Limitation en montant pour une carte de paiement sur une période donnée 9 : Limitation en nombre de transactions pour une carte de paiement sur une période donnée 11 : Limitation en nombre de transactions par alias sur une période donnée 12 : Limitation en montant par alias sur une période donnée 13 : Limitation en montant par IP sur une période donnée 14 : Limitation en nombre de transactions par IP sur une période donnée 15 : Testeurs de cartes 16 : Limitation en nombre d'alias par carte de paiement	
<valeur>	Données ayant engendrées le blocage	Entre les balises <analyse>
<couleur>	1 : Vert 2 : Orange 3 : Rouge	Entre les balises <scoring>
<action>	1 : Pas d'action : cinématique classique 2 : Désactivation 3DS (uniquement si option 3DS débrayable) 3 : Forçage 3DS 4 : Refus de la commande	Entre les balises <scoring>

3.4.2 Liste des valeurs du code retour dans les messages XML (balise <cdr>)

Valeur balise <cdr>	Description	Commentaire
0	Paiement non effectué	l'autorisation de l'émetteur n'a pas été délivrée
1	Conclusion effectuée	l'autorisation de l'émetteur a été délivrée et la Conclusion a été effectuée.

2	Résultat de l'étape 1 pour une carte enrôlée 3DSecure	le commerçant devra effectuer les étapes 2 et 3 pour l'authentification du client
-1	Problème technique	problème technique, il faut réitérer la demande
-2	Commerçant non identifié	les paramètres servant à identifier le site commerçant ne sont pas corrects, vérifier les champs societe, lgue et TPE
-3	Commande non authentifiée	la signature MAC est invalide
-4	carte de paiement expirée	la date de validité de la carte de paiement n'est pas valide
-5	Numéro de carte de paiement erroné	le numéro de la carte de paiement n'est pas valide
-6	Commande expirée	la date de la commande dépasse le délai autorisé (+/- 24h)
-7	Montant erroné	le montant transmis est mal formaté ou est égal à zéro
-8	Date erronée	la date transmise est erronée
-9	CVX erroné	le cryptogramme visuel transmis est erroné
-10	Paiement déjà autorisé	une autorisation a déjà été délivrée pour cette demande de paiement, il est toujours possible de conclure le paiement
-11	Paiement déjà accepté	le paiement relatif à cette commande a déjà fait l'objet d'une conclusion
-12	Paiement déjà annulé	la commande a été annulée et ne peut plus accepter de nouvelle demande d'autorisation
-13	Traitement en cours	la commande est en cours de traitement
-14	Commande grillée	le nombre maximal de tentatives de fourniture de carte a été atteint (3 tentatives sont acceptées), la commande n'est plus acceptée par le serveur Monetico
-15	Erreur paramètres	les paramètres transmis à l'émulation TPE sont erronés
-16	Erreur résultat d'authentification 3D-Secure	le résultat d'authentification 3D-Secure transmis à l'émulation TPE est invalide

-17	Le montant des échéances est erroné	Le montant des échéances transmis est mal formaté. La somme des échéances n'est pas égale au montant de la commande.
-18	La date des échéances est erronée	L'une des dates transmise est mal formatée. La différence entre les dates n'est pas d'un mois.
-19	Le nombre d'échéance n'est pas correct	Le nombre d'échéance doit être compris entre 2 et 4.
-20	La version envoyée n'est pas correcte	La version doit être égale à « 3.0 »
-21	Le paiement a été bloqué par filtrage	Les raisons du blocage sont présents dans la balise « filtrage ».
-22	carte de paiement séquestrée expirée	La date de la carte séquestrée utilisée est expirée
-23	Le paiement a été bloqué par scoring	Les raisons du blocage sont présents dans la balise « scoring ».
-24	CVV non présent	Le CVV n'a pas été fourni et est obligatoire
-25	TPE fermé	Le TPE utilisé est fermé
-26	AVS manquant	« Address Verification System » : l'adresse n'a pas été fournie
-27	Réseau de la carte de paiement non accepté	Le réseau de la carte de paiement n'est pas accepté par Desjardins ou par le commerçant

3.4.3 Cas où l'option « detailrefus » est activée

Balise	Description	Remarque
<cdr>	code retour	notez bien que si <cdr> est différent de 1, le paiement n'a pas été effectué
<version>	numéro de version du message de retour de l'émulation	Version courante 2.0 (3.0 si module antifraude activé)
<reference>	référence de la commande	

<aut>	numéro d'autorisation	<aut> n'est présent que si le paiement a été accepté
<phonie>	autorisation refusée pour un motif du type "appel phonie"	<phonie> n'est présent que si le champ "phonie" était présent et renseigné dans la requête appelante
<veres>	résultat d'enrôlement 3D-Secure Y : carte enrôlée 3D-Secure N : carte non enrôlée 3D-Secure U : problème technique	
<pares>	résultat d'authentification du client sur le serveur d'authentification de l'émetteur de sa carte Y : client authentifié N : client non authentifié A : la demande d'authentification a été effectuée et l'émetteur assume l'authentification du client U : non authentifié suite à un problème technique	<pares> n'est présent que si le commerçant a effectué un deuxième appel à l'émulation TPE suite à l'authentification du client
<pareq>	message complet à envoyer tel quel au serveur d'authentification de l'émetteur de la carte, pour l'authentification du client	<pareq> n'est présent que si le code retour <cdr> est égal à 2
<urlacs>	URL du serveur d'authentification de l'émetteur de la carte	<urlacs> n'est présent que si le code retour <cdr> est égal à 2
<md>	"Merchant Data" : le commerçant devra fournir telle quelle cette valeur au serveur d'authentification de l'émetteur de la carte.	<md> n'est présent que si le code retour <cdr> est égal à 2
<originecb>	Code pays de l'émetteur de la carte de paiement (norme ISO 3166-1)	<originecb> est présent pour un <cdr> positif ou nul

<hpancb>	Hachage irréversible (HMAC-SHA1) du numéro de la carte de paiement utilisée pour effectuer le paiement (identifiant de manière unique une carte de paiement pour un commerçant donné)	<hpancb> est présent pour un <cdr> positif ou nul
<filtrage>	Informations liées au filtrage du paiement	Uniquement présent lorsque le paiement a été bloqué
<scoring>	Informations liées au scoring du paiement	Uniquement présent lorsque le scoring est activé
<analyse>	Détails du blocage	Un groupe présent pour chaque filtre bloquant le paiement Entre les balises <filtrage> ou <scoring>
<cause>	Numéros des types de filtres bloquant le paiement (cf. tableau « Retours Module Prévention Fraude – détails » ci-dessous) 1 : Adresse IP 2 : Numéro de carte 3 : BIN de carte 4 : Pays de la carte 5 : Pays de l'IP 6 : Cohérence pays de la carte / pays de l'IP 7 : Liste noire 8 : Limitation en montant pour une carte de paiement sur une période donnée 9 : Limitation en nombre de transactions pour une carte de paiement sur une période donnée 11 : Limitation en nombre de transactions par alias sur une période donnée 12 : Limitation en montant par alias sur une période donnée 13 : Limitation en montant par IP sur une période donnée 14 : Limitation en nombre de transactions par IP sur une période donnée 15 : Testeurs de cartes 16 : Limitation en nombre d'alias par carte de paiement	Entres les balises <analyse>
<valeur>	Données ayant engendrées le blocage	Entre les balises <analyse>

<couleur>	1 : Vert 2 : Orange 3 : Rouge	Entre les balises <scoring>
<action>	1 : Pas d'action : cinématique classique 2 : Désactivation 3DS (uniquement si option 3DS débrayable) 3 : Forçage 3DS 4 : Refus de la commande	Entre les balises <scoring>
<motifrefus>	Motif du refus de la demande de paiement : Appel Phonie : l'émetteur de la carte demande des informations complémentaires Refus : l'émetteur de la carte refuse d'accorder l'autorisation Interdit : l'émetteur de la carte refuse d'accorder l'autorisation filtrage : la demande de paiement a été bloquée par le paramétrage de filtrage que le commerçant a mis en place dans son Module Prévention Fraude scoring : la demande de paiement a été bloquée par le paramétrage de scoring que le commerçant a mis en place dans son Module Prévention Fraude 3DSecure : si le refus est lié à une authentification 3DSecure négative reçue de l'émetteur de la carte du détenteur	Uniquement dans le cas où la demande de paiement a été refusée avec cdr=0

3.4.4 Liste des valeurs du code retour dans les messages XML (balise <cdr>)

Valeur balise <cdr>	Description	Commentaire
0	Paiement non effectué	l'autorisation de l'émetteur n'a pas été délivrée
1	Conclusion effectuée	l'autorisation de l'émetteur a été délivrée et la Conclusion a été effectuée.
2	Résultat de l'étape 1 pour une carte enrôlée 3DSecure	le commerçant devra effectuer les étapes 2 et 3 pour l'authentification du client
-1	Problème technique	problème technique, il faut réitérer la demande
-2	Commerçant non identifié	les paramètres servant à identifier le site commerçant ne sont pas corrects, vérifier les champs societe, lgue et TPE
-3	Commande non authentifiée	la signature MAC est invalide
-4	carte de paiement expirée	la date de validité de la carte de paiement n'est pas valide
-5	Numéro de carte de paiement erroné	le numéro de la carte de paiement n'est pas valide
-6	Commande expirée	la date de la commande dépasse le délai autorisé (+/- 24h)
-7	Montant erroné	le montant transmis est mal formaté ou est égal à zéro
-8	Date erronée	la date transmise est erronée
-9	CVX erroné	le cryptogramme visuel transmis est erroné
-10	Paiement déjà autorisé	une autorisation a déjà été délivrée pour cette demande de paiement, il est toujours possible de conclure le paiement
-11	Paiement déjà accepté	le paiement relatif à cette commande a déjà fait l'objet d'une conclusion
-12	Paiement déjà annulé	la commande a été annulée et ne peut plus accepter de nouvelle demande d'autorisation

-13	Traitement en cours	la commande est en cours de traitement
-14	Commande grillée	le nombre maximal de tentatives de fourniture de carte a été atteint (3 tentatives sont acceptées), la commande n'est plus acceptée par le serveur Monetico
-15	Erreur paramètres	les paramètres transmis à l'émulation TPE sont erronés
-16	Erreur résultat d'authentification 3D-Secure	le résultat d'authentification 3D-Secure transmis à l'émulation TPE est invalide
-17	Le montant des échéances est erroné	Le montant des échéances transmis est mal formaté. La somme des échéances n'est pas égale au montant de la commande.
-18	La date des échéances est erronée	L'une des dates transmise est mal formatée. La différence entre les dates n'est pas d'un mois.
-19	Le nombre d'échéance n'est pas correct	Le nombre d'échéance doit être compris entre 2 et 4.
-20	La version envoyée n'est pas correcte	La version doit être égale à « 3.0 »
-22	carte de paiement séquestrée expirée	La date de la carte séquestrée utilisée est expirée
-24	CVV non présent	Le CVV n'a pas été fourni et est obligatoire
-25	TPE fermé	Le TPE utilisé est fermé
-26	AVS manquant	« Address Verification System » : l'adresse n'a pas été fournie
-27	Réseau de la carte de paiement non accepté	Le réseau de la carte de paiement n'est pas accepté par Desjardins ou par le commerçant

3.4.5 Retours Module Prévention Fraude – Détails

La fonctionnalité de filtrage des paiements s'appuie sur un ensemble de neuf filtres, librement paramétrable sur le tableau de bord (nouvelle version). Chacun de ces filtres agit sur un critère spécifique, comme l'adresse IP du client, son adresse email, le pays de sa carte de paiement…

Numéro du type de filtre	Critère d'analyse	Valeur retournée comme raison du blocage	Remarque
1	Adresse IP	Adresse IP du client	
2	Numéro de carte	Hash de la carte du client	Fonctionne uniquement pour les paiements par carte
3	BIN de carte	Bin de la carte du client	
4	Pays de la carte	Pays de la carte du client	
5	Pays de l'IP	Pays de l'IP du client	
6	Cohérence pays de la carte / pays de l'IP	Pays de la carte # Pays de l'adresse IP du client	Fonctionne uniquement pour les paiements par carte
7	Liste noire	Nom de domaine de l'adresse email du client	
8	Limitation en montant pour une carte de paiement sur une période donnée	Montant cumulé en CAD sur la période donnée associé à la carte du client	Fonctionne uniquement pour les paiements par carte
9	Limitation en nombre de transactions pour une carte de paiement sur une période donnée	Nombre de transactions cumulées sur la période donnée associée à la carte du client	
11	Limitation en nombre de transactions par alias sur une période donnée	Nombre de transactions cumulées sur la période donnée associée à l'alias du client	Uniquement en cas de souscription de l'option paiement express
12	Limitation en montant par alias sur une période donnée	Montant cumulé en CAD sur la période donnée associé à l'alias du client	

13	Limitation en montant par IP sur une période donnée	Montant cumulé en CAD sur la période donnée associé à l'adresse IP du client	
14	Limitation en nombre de transactions par IP sur une période donnée	Nombre de transactions cumulées sur la période donnée associée à l'adresse IP du client	
15	Testeurs de cartes	Nombre de transactions cumulées sur la période donnée associée à l'adresse IP du client	
16	Limitation en nombre d'alias par carte de paiement	Les alias déjà associés à la carte utilisée pour le paiement	Uniquement en cas de souscription de l'option paiement express Fonctionne uniquement pour les paiements par carte.

4 Annexes

4.1 Contraintes générales de codage HTML des champs

Tous les champs de la requête d'appel, à l'exception de la version et du montant, doivent être codés en HTML avant la mise en forme dans le formulaire (c'est à dire immédiatement après le calcul du MAC).

Les caractères à coder impérativement sont les codes ASCII de 0 à 127 réputés risqués :

Nom	Symbole	Remplacement
Signe Commercial	&	&amp;
Signe inférieur	<	&lt;
Signe supérieur	>	&gt;
Guillemets	"	" ou "
Apostrophe	'	&#x27;

Les fonctions de type « HTML_ENCODE » (cf. IETF RFC1738) des langages conviennent parfaitement, elles encodent beaucoup plus de caractères, typiquement tout ce qui n'est pas :

- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- abcdefghijklmnopqrstuvwxyz
- 0123456789
- _ . - (souligné, point, tiret)

Si vous utilisez dans le champ « texte-libre » des caractères hors de la plage ascii commune imprimable (31<ascii<127), vous devez coder ce champ avant tout traitement relatif au paiement pour éviter tout problème de calcul du sceau MAC.

Enfin, les champs ne doivent pas contenir les caractères ASCII 10 et ASCII 13 (CR et LF).

4.2 Contraintes particulières selon le champ

Champs	Contenu / format avant codage HTML	Taille maximale après codage HTML
TPE	A-Z a-z 0-9	**7**
version	3.0	**Fixe**
date		**50**
montant		**20**
référence	A-Z a-z 0-9	**12**
MAC	0-9 A-F a-f	**40**
lgue	A-Z	**2**
societe	A-Z a-z 0-9	**50**
texte-libre	Base 64	**3200**
numero_carte	0-9	**16**
annee_validite	0-9	**4**
mois_validite	0-9	**2**
cvx	0-9	**3**
phonie	A-Z a-z 0-9	**50**
mail		**50**
nbrech	2-4	**1**
dateechN		**50**
montantechN		**20**
option=clientip	0-255.0-255.0-255.0-255	**25**
option=detailrefus	0-1	**1**

4.3 Explication du mode 3D-Secure

4.3.1 Principe

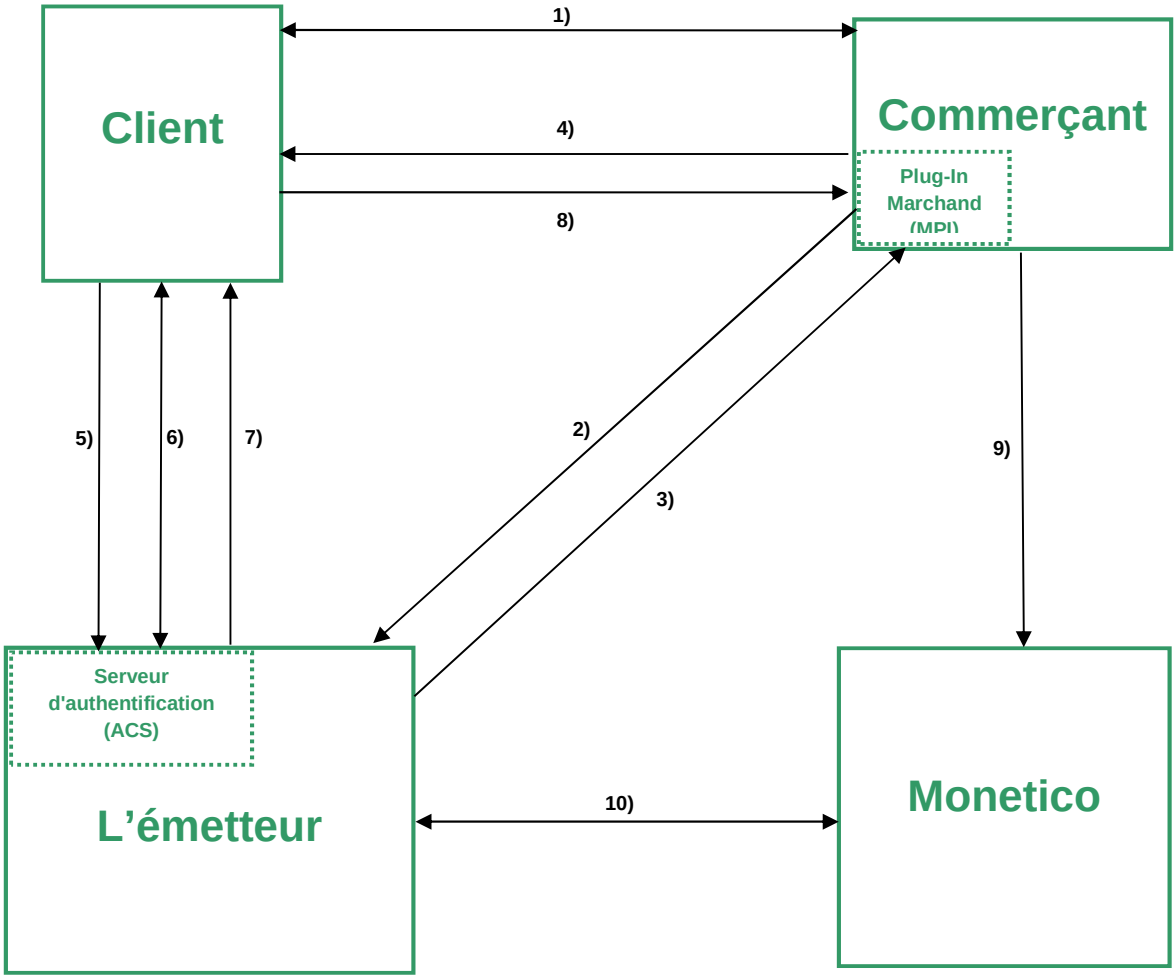
Afin de renforcer la sécurité des transactions sur internet, une nouvelle norme de sécurité est désormais en place : le 3D Secure. Elle a pour but de réduire les risques de fraude, grâce une procédure d'authentification du détenteur de la carte auprès de son émetteur.

Un objectif : diminuer les risques de fraude

Afin d'éviter qu'une transaction soit rejetée parce que le client conteste l'achat auprès de son émetteur, celle-ci vérifie désormais l'identité du client. En plus du numéro, de la date de validité et du cryptogramme, avec le système 3D Secure, le détenteur de la carte doit s'authentifier auprès de son émetteur en lui fournissant un code ou une information personnelle.

4.3.2 Fonctionnement

Voici le synoptique simplifié des échanges en mode 3DSecure :


Client
Commerçant
Plug-In
Marchand
(MPI)
Serveur
d'authentification
(ACS)
L'émetteur
Monetico
1)
2)
3)
4)
5)
6)
7)
8)
9)
10)

Etape	Description
Etape 1	Le client réalise ses achats sur le site internet du commerçant, et saisit son numéro de carte de paiement, la date d'expiration et le cryptogramme visuel.
Etape 2	Le plug-in marchand (MPI) envoie une requête de vérification d'enrôlement de la carte de paiement du client (VEReq) au serveur d'authentification de l'émetteur de la carte (ACS).
Etape 3	Le serveur d'authentification de l'émetteur de la carte soumet le résultat d'enrôlement (VERes) au MPI. Si la carte de paiement du client n'est pas enrôlée 3D-Secure, une demande d'autorisation est effectuée, et les étapes 4 à 9 sont ignorées.
Etape 4	Le MPI envoi une requête d'authentification (PAReq) via le navigateur du client à l'ACS.
Etape 5	L'ACS reçoit la requête d'authentification (PAReq).
Etape 6	L'ACS procède à l'authentification du client.
Etape 7	L'ACS soumet le résultat d'authentification du client (PARes) au MPI via le navigateur du client.
Etape 8	Le MPI reçoit le résultat d'authentification du client (PARes).
Etape 9	La demande d'autorisation en mode "3D-Secure" est alors réalisée.
Etape 10	La transaction est effectuée.

4.3.3 Glossaire 3D-Secure

Terme	Description
ACS	Serveur sécurisé d'authentification 3D-Secure.
VEReq	Requête pour la vérification de l'enrôlement d'une carte de paiement en 3D-Secure.
VERes	Résultat d'enrôlement d'une carte de paiement en 3D-Secure.
PAReq	Requête d'authentification du client.
PARes	Résultat de la requête d'authentification du client.
MPI	Plug-in marchand : module logiciel qui permet de vérifier l'enrôlement 3D-Secure d'une carte de paiement et de retourner l'adresse du site Web du serveur d'authentification de l'émetteur de la carte du détenteur.

5 Utilisation du service

5.1 En Test

Le rôle de notre serveur de test est de vous permettre de tester et de valider vos développements.

Sur ce serveur, le seul contrôle effectué est un contrôle de structure du numéro de carte. Il n'y a pas d'autres contrôles effectués : date d'expiration, contrôle du fichier des cartes en opposition, etc., comme cela existe sur notre serveur de paiement de production.

Bien sûr, aucun paiement accepté par notre serveur de paiement de test ne donne lieu à une Conclusion.

Afin de tester les différents codes de retour du serveur Monetico, vous avez la possibilité d'utiliser plusieurs cartes de tests dont les autorisations de l'émetteur sont différentes :

Numéro de carte	Autorisation
0000 0100 0000 0001	**Carte non enrôlée 3D-Secure avec autorisation refusée**
0000 0100 0000 0002	**Carte non enrôlée 3D-Secure avec autorisation acceptée**
0000 0100 0000 0003	**Carte non enrôlée 3D-Secure avec appel phonie**
0000 0100 0000 0004	**Carte enrôlée 3D-Secure non authentifiée avec autorisation refusée**
0000 0100 0000 0005	**Carte enrôlée 3D-Secure authentifiée avec autorisation acceptée**
0000 0100 0000 0006	**Carte enrôlée 3D-Secure authentifiée avec autorisation refusée**

L'environnement de test est disponible à l'adresse suivante :

- https://p.monetico-services.com/test/emulation3ds.cgi

5.2 En Production

Après avoir validé vos développements, vous pourrez vous adresser au serveur de production, disponible à l'adresse suivante :

- https://p.monetico-services.com/emulation3ds.cgi

Nous attirons votre attention sur le fait que les requêtes de paiement adressées au serveur de production seront des paiements réels.

5.3 Assistance technique

Desjardins propose une assistance à la compréhension générale de l'utilisation de sa solution :

- Par courriel : support@desjardins.monetico-services.com
- Par téléphone :
  Montréal et les environs : 514 397-4450
  Canada et États-Unis : 1 888 285-0015

Cependant, Desjardins n'offre qu'un soutien limité concernant les problématiques d'intégration technique de sa solution de paiement dans le système d'information commerçant.

FIN DU DOCUMENT

.